Amendments to the Specification:

Please replace page 2, paragraph 1, of the specification:

a1

Security, particularly data security, is an essential aspect of any computer and its operating system ~~can provide address that security~~. It is desirable to make data and programs stored on a computer system available to authorized users with a minimum of effort by (and delay to) an authorized user with minimum overhead to the computer while preferably denying access to the programs and data to those who are not authorized to use the data and programs (or at least delaying substantially and requiring much time and trouble).

Please replace page 5, paragraph 2, of the specification:

a2

The present invention also maintains a log of the attempt to access the personal computer and the results of those attempts, so that access may be terminated when a predetermined threshold of unsuccessful password attempts has been reached. The log can be queried to determine whether suspicious patterns of activity have been encountered and, based on the log of successful password attempts, it may be able to determine whether the security of the personal[[;]] computer (particularly it data and programs) has been breached.

Please replace pages 7-8, paragraph 3 of the specification:

a3

The System Owner is the user who is [[us]] responsible for the configuring and placing the system in the secured mode initially. The System Owner will control configuration both initially and whenever an update needs to be made. The System Owner will control the Security Password and be responsible for maintaining its integrity. The System Owner will maintain physical security of a tamper-evident cover key lock. The System Owner will be responsible for maintaining security logs on all systems. The System Owner will also have to maintain a record of all attempted security breaches. The System Owner may own more than one system. The System Owner is considered an authorized user and can also be considered a normal user.

Please replace pages 11-12, paragraph 2, of the specification:

a4

Fig. 1 is a pictorial view of a personal computer 10 useful in practicing the present invention. The personal computer 10 includes a display 11 coupled to a system unit 12, with a keyboard 14 attached to the system unit 12. Additionally shown in this Fig.1, although optional in face, are a mouse 16 for user input and a printer 18 for providing printed output from the personal computer 10. Not shown in this Figure, but well known in the art, the personal computer 10 may be connected, either through some standard attachment or through a modem, to a network and may include a variety of temporary and permanent memory and storage in the form of random access memory (RAM), read only memory (ROM) and disk storage, either in the form of one or more hard drives or one or more drives with removable media such as CD-ROMS's and floppy diskettes. The data and programs stored in a personal computer have value to the other and to a4 cont

others who want to have access to the data (and sometimes to a lesser extent, the programs), and it is to reduce the likelihood of access to such programs and data that the present invention is addressed. The system unit 12 includes 13 which surround the storage and processor, covers which may be secured against tampering by a key lock and/or tamper indicating circuitry.

Please replace page 13, paragraph 2, of the specification:

A system in its most secure state when access is only granted to a level 0 person. A system [[it]] is in its [[it]] least secure state when access is granted to a level 4 person.

a5

[Please replace pages 13-14, paragraph 3 of the specification:]

Fig. 3 is a flow chart illustrating the process of the present invention, which begins at block 40, illustrating the start of the Power-On-System-Test (POST). Thereafter, the process passes to block 42 which illustrates normal POST operations. Next, the process passes to block 44, which depicts a determination of whether or not an attempt has been made to decrease security. If so, the process passes to block 46 which depicts a determination of whether or not the proper security password has been entered. If the proper security password has not been entered, the process passes to block 48. Block 48 illustrates a denial of the attempted change in the security profile.

Referring again to block 44, in the event no attempt has been made to decrease security, or, referring to block 46, in the event an attempt to decrease security has been made and the entered security password was correct or, the entrance security password was incorrect and the security profile change was denied, the process passes to block 50. Block 50 illustrates the setting up of the security profile.

Next, the process passes to block 52, which illustrates the continuing of normal POST operations. Block 54 depicts the ending of POST operations and the booting of the operating system. Thereafter, block 56 depicts normal operating system operations.

Block 58 of the flow chart of Figure 3 illustrates a user requesting a security change and the process then passes to block 60. Block 60 depicts a determination of whether the user desires to increase security, and if so, the process passes to block 64, which illustrates a denial of the change in profile. If not, the process passes to block 62, which depicts a change in the security profile. Thereafter, the process passes to block 66, which illustrates a continuation of normal operating system operations.

Thus, [[D]]during the power-on-self-test, the security profile can be written and read as desired, but after POST is completed, a normal user can only write ones into the security profile. Thus, the memory is all ones in its most secure state and all 0's when it is in its least secure states. This has the advantage that, should power be lost the personal computer for long enough to drain the power, the system will default to all ones or its most secure state. Of course, the security profile can be updated (e.g., by the System Owner) using his privilege password (e.g. the PAP or PA) to make the security profile less secure, if desired. Since some of the fields (such as the tamper evident field) may be programmed to shut the personal computer down to normal users, it would be essential that there be a mechanism available to someone to reverse such fields, but this is a privilege of a super-user or system owner and not permitted to a normal user. Because, if ~~If~~ a normal user attempted unsuccessfully to give himself the rights of a System Owner, for example, or other privilege, he would like to erase any ~~the~~ record of such attempt ~~attempts~~, while the System Owner would certainly wish to preserve an ~~the~~ indication of such unauthorized activity.

a5 cont

[Please replace page 13, paragraph 3 of the specification:]

Fig. 3 is a flow chart illustrating the process of the present invention. During the power-on-self-test, the security profile can be written and read as desired, but after POST is completed, a normal user can only write ones into the security profile. Thus, the memory is all ones in its most secure state and all [[0's]] zeros when it is in its least secure state. This has the advantage that, should power be lost to the personal computer for long enough to drain the power, the system will default to all ones or its most secure state. Of course, the security profile can be updated (e.g., by the System Owner) using his privilege password (e.g., the PAP or PA) to make the security profile less secure, if desired. Since some of the fields (such as the tamper evident field) may be programmed to shut the personal computer down to normal users, it would be essential that there be a mechanism available to someone to reverse such fields, but this is a privilege of a super-user or system owner and not permitted to a normal user. [[If]] Because, if a normal user attempted unsuccessfully to give himself the rights of a System Owner, for example, or other privilege, he would like to erase [[the]] any record of such attempt[[s]], while the System Owner would certainly wish to preserve [[the]] an indication of such unauthorized activity.

Please replace page 16, paragraph 2 of the specification:

a6

The second field 74 of the security profile 70 is a field which indicates then number of unsuccessful attempts at entering the user password that would be permitted before the system is shut down. In this example, 000 would equal 7, 001 would equal 6, [[,]] 010 would equal 5, 011 would equal 4, 100 would equal 3, 101 would equal 2, 110 would equal 1 and 111 would equal 0. The user would be permitted to attempt the number of permitted unsuccessful attempts plus one, to allow for a successful attempt at the end. This field could be set by an operating system API (for example, to take into account a greater security exposure during certain time periods, like late evening or on certain days, like weekends).